Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
United States Department of Justice,	)	
Federal Bureau of Investigation and	)	
Drug Enforcement Administration	)	
	)	RM-10865
Joint Petition for Rulemaking to Resolve	)	
Various Outstanding Implementation Issues	)	
Concerning the Implementation of the	)	
Communications Assistance for Law	)	
Enforcement Act	)	

COMMENTS OF COVAD COMMUNICATIONS

Jason Oxman
Assistant General Counsel

Praveen Goyal
Senior Counsel for Government & Regulatory Affairs

Covad Communications
600 14th St., NW Suite 750
Washington, DC 20005
(202) 220-0400

April 12, 2004

I. Introduction

Covad Communications, by its attorneys, herewith respectfully submits its comments in response to the Joint Petition for Rulemaking filed on March 10, 2004, by the U.S. Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration (collectively, "Petitioners") regarding implementation of the Communications Assistance for Law Enforcement Act.[1] Covad shares the Petitioners' belief that law enforcement should be able to conduct lawful intercepts of communications traversing broadband telecommunications networks. Covad also shares the Petitioners' belief that broadband telecommunications service providers should comply with their obligations to provide technical assistance capabilities to law enforcement for such intercepts. Indeed, as explained below, Covad regularly complies with lawful intercept orders it receives, with established internal procedures for enabling law enforcement access to Covad's network. Covad also agrees with the Petitioners that there is still much work to be done, by industry members, standards setting organizations and law enforcement agencies, to ensure that the requirements of CALEA are faithfully met for broadband telecommunications service networks.

Covad strongly disagrees, however, with the specific policy proposals made by the Petitioners. Covad believes that the Petitioners' proposals represent a vast overreach to institute unnecessary, burdensome new powers for law enforcement at the expense of innovation in the broadband space. Indeed, in many respects, the Petitioners' proposals resemble rehashes of policy positions law enforcement previously took and lost in the Commission's previous CALEA implementation proceedings. Covad believes the

[1] *See* Joint Petition for Expedited Rulemaking of the U.S. Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration in RM-10865, filed March 10, 2004 ("Joint Petition").

Commission should not allow the Petitioners to resurrect old policy fights they have already lost in years past, under the guise of implementing rules for new broadband technologies.

Covad is the leading nationwide provider of broadband connectivity using digital subscriber line (DSL) technology. Covad's nationwide facilities-based broadband network reaches the top 100 markets in the nation, comprising nearly half of the nation's homes and businesses. As a facilities-based provider, Covad purchases access to unbundled transmission facilities (loops and interoffice transport) from the ILEC to reach customers from its own broadband facilities, including Digital Subscriber Line Access Multiplexers (DSLAMs), IP routers, and ATM switches collocated in over 1800 ILEC central offices across the nation. As a facilities-based provider of broadband telecommunications services, Covad would be severely burdened by several of the Petitioners' proposals, which would greatly and unnecessarily hinder Covad's ability to deploy innovative technologies and services for its customers.

Covad shares the Petitioners' view of the vital importance of broadband intercept standards for law enforcement use in protecting homeland security. Indeed, as explained in detail below, law enforcement agencies already routinely obtain lawful intercepts of the broadband telecommunications traversing Covad's network. Thus, Covad urges the Commission to reject the sweeping new statutory reinterpretation called for by the Petitioners' proposals. Instead, Covad believes that the Commission can take measured steps to accelerate the deployment of CALEA-compliant intercept standards for broadband service providers, steps that will improve the current abilities of law enforcement agencies to lawfully access broadband communications services, without

unduly burdening broadband carriers and the consumers they serve. Accordingly, instead of the Petitioners' broadly sweeping proposals, Covad urges the Commission to adopt the more moderate measures recommended below.

II. The Rollout of Broadband Telecommunications Services Has Not Blocked Law Enforcement Access to Lawful Intercepts

Petitioners claim that, because their proposals are not yet in place, "the ability of federal, state and local law enforcement to carry out critical electronic surveillance *is being compromised today* by providers who have failed to implement CALEA-compliant intercept capabilities."[2] What the Petitioners neglect to mention, however, is that even today providers of so-called packet-mode services routinely comply with lawful intercept orders. Even Covad, whose telecommunications services are comprised exclusively of packet-switched, broadband data services, regularly enables law enforcement access to the data communications traversing its network pursuant to lawful intercept orders.

Indeed, Covad trains its employees and provides them with process policies to follow in the event law enforcement makes an information request about an end-user's communications. Under Covad's processes, law enforcement can access information about both the "Layer 2" (e.g., Ethernet, ATM) and "Layer 3" (e.g., IP) services Covad provides for individual end user circuits.[3] If required under the terms of a lawful intercept order, Covad's policies include processes for allowing law enforcement agents to "wire-tap" individual end-user circuits by connecting them to law enforcement agencies' installed equipment, as well as processes for "content capture" to supply law

[2] *See* Joint Petition at 8.

[3] "Layer 2" and "Layer 3" refer to the 7-layer Open System Interconnection, or OSI, model. Layer 2 commonly refers to the Data Link or Logical Link Layer (e.g., Ethernet, ATM), while Layer 3 commonly refers to the Network Layer (e.g., Internet Protocol). Covad is both a retail provider as well as a wholesale provider of broadband telecommunications services, and provisions both Layer 2 and combined Layer 2-Layer 3 services over individual end user circuits.

enforcement agencies with copies of hosted content (e.g., email, web) for individual end users.[4] Thus, Covad has regularly worked with law enforcement agencies to ensure that requests for end user information (e.g., intercept requests pursuant to subpoena or court order) are satisfied.

Would it be better for the industry to develop a standard means of complying with law enforcement intercept requests? Unquestionably, the right packet-mode intercept standard should lead to more efficient use of both carrier and law enforcement resources in complying with CALEA requests than any current ad hoc processes already in place. In fact, as discussed below, the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS) recently announced their release of published standards for lawfully authorized electronic surveillance, in a revised version of the "J-standard" (J-STD-025-B).[5] Their work, now culminated in a published standard, demonstrates that the industry standards setting process is working. But, even until such standards are in place, law enforcement can hardly claim, at least with respect to Covad, that the needs of law enforcement to access broadband communications services are simply not being met at all.

III. The Number of Packet-Mode Compliance Extensions Already Granted Is No Basis for Adopting Petitioners' Proposals

In support of their contention that law enforcement needs for surveillance of broadband communications are simply not being met, the Petitioners recite a litany of extensions the Commission has granted for packet-mode CALEA compliance by carriers

[4] Although, as discussed below, information services are not subject to CALEA's technical requirements and assistance capability requirements, the Commission has also made clear that information services may nonetheless be accessed by law enforcement agencies under a lawful court order independent of CALEA's assistance capability requirements. *See infra* at pp. 10-11.

[5] *See* "TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Standard (J-STD-025-B)," Press Release, Mar. 19, 2004, http://www.tiaonline.org/media/press_releases/index.cfm?parelease=04-26.

that do not yet have in place packet-mode interception capabilities.[6] Whether or not all of these extensions were appropriately granted is not an issue for Covad to second-guess. While Covad has been able to implement an interim mechanism for law enforcement to access its own broadband network, Covad is not in a position to determine whether other carriers are or are not similarly capable of instituting such interim measures. The fact that the Petitioners rely on these numerous compliance extensions as one of the main bases for their petition, however, does reveal the curious illogic in their proposals.

As the Petitioners' rightly recognize, *there already exists a requirement to provide packet-mode intercept capabilities.* Specifically, in 1999, the Commission adopted an interim standard for packet-mode intercept capabilities, without requiring a specific technical standard for packet-mode intercept capability.[7] As the Commission recognized as far back as 1999, the effect of adopting its interim standard rather than specific technical requirements was to allow law enforcement to access more information about end users' communications than they might be entitled to.[8] Under the Commission's current rules, that general requirement has been in force since November 19, 2001.[9] Thus, the Petitioners' problem does not appear to be the absence of a packet-mode intercept requirement. Their problem appears to be that it has not been sufficiently enforced, in their view.

---

[6] *See* Joint Petition at 35, n. 62.

[7] *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Third Report and Order, FCC 99-230 (*CALEA Third Report and Order*) (1999) (adopting technical requirements for most CALEA intercept capabilities, but adopting only an interim standard for packet-mode intercept capabilities without technical requirements).

[8] Specifically, the Commission recognized that under the interim standard, law enforcement agencies might be able to access both call identifying information and call content for packet-mode services under a pen register order. *See id.* at para. 56.

[9] *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Order, FCC 01-265 (*CTIA Packet-Mode Compliance Extension Order*) (2001) (extending deadline for packet-mode compliance under interim standard in J-STD-025 until November 19, 2001).

In that case, if the volume of packet-mode compliance extensions the Commission grants is the root of law enforcement's supposed inability to lawfully intercept broadband communications, the Petitioners beg the question of how exactly the proposals in their Joint Petition would solve that problem. If the great majority of carriers simply cannot implement packet-mode intercept capabilities, how does now creating a requirement that they do it in the next 15 months get them any closer to having that capability? After all, the same carriers had 15 months to implement packet-mode intercept capabilities under the interim standard the first time around in 1999, and that doesn't seem to have taken place.[10] There is nothing in the Joint Petition that would actually make it any easier or faster for carriers to implement packet-mode intercept capabilities – for example, by recommending a specific intercept standard for industry review.

On other hand, perhaps the Petitioners are really concerned that the great majority of the carriers receiving the complained-of extension grants actually can implement interim measures to comply with the interim packet-mode compliance standard, notwithstanding the many extension requests routinely granted. In this case, rather than rewriting the CALEA statute, the solution would be to simply *enforce the packet-mode intercept requirement already in place*. In other words, the Petitioners might believe that the Commission should deny some of the compliance extensions it has previously granted. Of course, Covad believes that carriers that cannot actually technically comply with the existing packet-mode intercept requirement should not and cannot be forced to do so. Furthermore, Covad takes no position on whether or not any individual extension request in the past was appropriately granted – that is a matter between individual

[10] *See CALEA Third Report and Order* at para. 55.

petitioning carriers and this Commission. The point, however, is that the Petitioners' concerns about the volume of extension requests routinely granted should be addressed by examining the merits of those requests themselves – not by granting new, unrelated powers to law enforcement.

Indeed, if the Petitioners believe, as they appear to imply with their aggressive 15 month packet-mode intercept solution deployment schedule, that a great number of the carriers currently receiving extensions can actually offer interim packet-mode intercept capabilities, their Petition could have focused on demonstrating how carriers could offer such capabilities. For example, the Petitioners could have offered individual examples of such intercept solutions for classes of carriers currently applying for and receiving extensions. However, instead of offering constructive proposals for carriers to implement such interim measures and come into compliance with existing packet-mode requirements, the Petitioners appear to seek only the creation of onerous, unrelated new requirements.

IV. CALEA Should Not and Need Not Be Construed to Apply to Information Services, including VoIP Applications, to Enable Lawful Intercepts

Although the Petitioners' real complaint appears to be about the number of carriers that have received extensions from the Commission for compliance with the Commission's existing packet-mode compliance requirement, their specific proposals go far beyond remedying this problem. Instead, the Petitioners list a series of products and services to which CALEA's statutory assistance capability and technical requirements clearly do not apply[11] – including products and services which do not even exist yet. Specifically, the Petitioners attempt to blur the lines between the Communications Act's

[11] *See* 47 U.S.C. §§ 1002, 1006.

definitions of "telecommunications services" and "information services" respectively – notwithstanding the Commission's clear previous findings to the contrary. Ultimately, the Petitioners would have the Commission upend the entire analytical framework the Commission has applied since 1999 to determine which services and entities are subject to CALEA's requirements – reopening debates the Commission already conclusively settled in the *CALEA Second Report and Order.*

According to the Petitioners, CALEA's requirements apply to all "telecommunications carriers," a term that, according to the Petitioners, under CALEA has its "own, broader, statutory definition" than the identical term in section 3 of the Communications Act.[12] Of course, the Petitioners are correct that Title 47 in two places defines the term "telecommunications carrier" – in both section 3 of the Act as well as section 1001.[13] The Petitioners are also correct that both definitions contain different provisions – a fact that led the Commission to conclude, as the Petitioners rightly point out, that "the entities and services subject to CALEA must be based on the CALEA definition … independently of their classification for the separate purposes of the Communications Act."[14] Unfortunately, the Petitioners omit from this out-of-context quotation the Commission's qualification of this otherwise broad statement: "*we expect in virtually all cases that the definitions of the two Acts will produce the same results*…".[15] In other words, the Commission recognized that, as a formal matter, section 3 and section 1001 of Title 47 each contain different language defining

---

[12] *See* Joint Petition at 9.

[13] *See* 47 U.S.C. § 3(44); §1001(8).

[14] *See* Joint Petition at 9 (quoting *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Second Report and Order, FCC 99-229, ¶ 13 (1999) (*CALEA Second Report and Order*)).

[15] *CALEA Second Report and Order* at para. 13.

"telecommunications carrier," but recognized that the definitions were so similar that it expected both provisions to apply to the same entities "in virtually all cases."

As the Joint Petition makes clear, the reasons for the Petitioners' re-definition of "telecommunications carrier" is to sweep into CALEA's ambit services ordinarily considered "information services" under the Act – in direct contravention of the Commission's previous findings in the *CALEA Second Report and Order*. In that Order, the Commission made clear that information services are not subject to CALEA's assistance capability requirements, as the express language of CALEA itself makes clear.[16] Indeed, the Commission's *Second Report and Order* maintained a clear line between telecommunications services and facilities subject to CALEA's assistance capability requirements, and the information services and facilities not subject to CALEA's assistance capability requirements:

> Where facilities are used solely to provide an information service, whether offered by an exclusively-IS provider or by a common carrier that has established a dedicated IS system apart from its telecommunications system, we find that such facilities are not subject to CALEA. Where facilities are used to provide both telecommunications and information services, however, such joint-use facilities are subject to CALEA in order to ensure the ability to surveil *the telecommunications services*.[17]

In other words, the fact that information services are offered over a telecommunications service network in no way obviates the underlying carrier's obligation to meet section 1002's assistance capability requirements, to ensure that law enforcement agencies have the ability to surveil the telecommunications service traffic traversing that network.

---

[16] *See* 47 U.S.C. § 1002(b)(2)(A).

[17] *CALEA Second Report and Order* at para. 27. Of particular relevance to Covad, the Commission went on to offer an example of such "joint-use" facilities: "For example, digital subscriber line (DSL) services are generally offered as tariffed telecommunications services, and therefore subject to CALEA, even though the DSL offering often would be used in the provision of information services." *Id.*

The Petitioners' attempt to sweep information services into the ambit of CALEA is doubly troubling given the express prohibition in CALEA against doing so[18] – and given that both CALEA and section 3 of the Act contain virtually identical definitions of "information services."[19] Their reasons for attempting to sweep information services into the ambit of CALEA are obvious – to impose upon providers of information services, such as VoIP applications, the same technical requirements and assistance capability requirements that apply to the underlying telecommunications carriers over whose networks such services are offered. The Petitioners make clear that their wide swath of targets includes, but is not limited to, "broadband access service and broadband telephony service" – including stand-alone broadband telephony services not containing a broadband access component.[20]

What is less clear from the Joint Petition is why this wide expansion of CALEA's sweep to include information service providers heretofore generally considered exempt from CALEA is even necessary. As an initial matter, the Commission has previously made clear that, notwithstanding the exemption of information services from compliance with CALEA itself, wiretaps of information services are still available to law enforcement under a lawful court order. As the Commission recognized in the *CALEA Second Report and Order*:

> …[I]nformation services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements [in CALEA].[21]

---

[18] *See* 47 U.S.C. § 1002(b)(2)(A).

[19] *Cf.* 47 U.S.C. § 3(20); § 1001(a)(6).

[20] *See* Joint Petition at 15-16 and n. 39.

[21] *See Second Report and Order*, para. 12 (quoting legislative history in H.R. Rep. No. 103-827(I), at 21, reprinted in 1994 U.S.C.C.A.N. 3489, 3498).

In other words, like any other entity, information service providers such as VoIP providers must comply with the terms of any lawful court order, including one requiring them to provide an intercept of their information services. The only thing CALEA exempts information service providers from doing is designing their applications and systems to meet the assistance capability requirements that apply to telecommunications carriers in section 1002 of CALEA.

Furthermore, and more fundamentally, it remains unclear from the Joint Petition why law enforcement even needs information services providers, including providers of applications such as VoIP, to design their applications and systems to comply with CALEA – given that end users must subscribe to telecommunications services in order to access and use such information services in the first place. In other words, why isn't the CALEA compliance of the underlying telecommunications carrier sufficient to enable law enforcement access to any information services content traveling over the underlying carrier's network? To give an example, Covad is a broadband telecommunications carrier subject to CALEA's assistance capability requirements. Why isn't law enforcement's access, facilitated under CALEA, to the identifying information and content of traffic flowing over Covad's network (including data generated by or destined for information services, such as VoIP applications), in conjunction with law enforcement's subpoena power to access the records and systems of information service providers offering services over Covad's network, sufficient to provide law enforcement with the access it needs? The Petitioners fail to explain why this set of existing requirements, if properly enforced, would be insufficient to meet the legitimate needs of law enforcement. Instead, they demand the extension of CALEA's requirements to new

categories of information service providers, requirements they simultaneously complain have failed to be implemented in the first place.

Similarly, the Petitioners would have the Commission create new presumptions of CALEA coverage, according to broad criteria set forth by the Petitioners, criteria which make no mention of the distinction the Commission and the statute draw between covered telecommunications services and exempt information services.[22] According to the Petitioners, a new service should be presumed to fall under CALEA whenever it competes with any existing service covered by CALEA.[23] The Petitioners might have been thinking of VoIP applications in crafting these criteria. However, particularly after the Commission's *Triennial Review Order*, not even the provisions of CALEA defining "telecommunications carriers" to include services that replace "a substantial portion of the local telephone exchange service" seem to save this interpretation.[24] It is hard to see how current VoIP services substitute for traditional local telephone exchange services when the Commission has determined that cable telephony and CMRS services do not.[25]

Indeed, would email be required to offer CALEA assistance capabilities, or instant messaging services for that matter? Many people do substitute those for traditional circuit switched long distance services. How about instant messaging services

---

[22] *See* Joint Petition at 33-34.

[23] *See* Joint Petition at 33.

[24] *See* 47 U.S.C. § 1001(8)(B)(ii).

[25] In the *Triennial Review Order*, the Commission explained that it did not consider cable telephony services and CMRS services to constitute true alternatives to the incumbent local exchange telephone services in a given market. *See Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers,* CC Docket Nos. 01-338, 96-98, and 98-147, Report and Order and Order on Remand and Further Notice of Proposed Rulemaking, FCC 03-36, at paras. 444-46 (2003). Cable telephony subscribers number around 2.6 million homes in the U.S., *see id.* at para. 444, while CMRS subscribers number around 148 million subscribers, *see* "Local Telephone Competition: Status as of June 30, 2003," Industry Analysis and Technology Division of the Wireline Competition Bureau, Federal Communications Commission (rel. Dec. 2003). If these services are not substitutes for local telephone exchange services, it is hard to see how current VoIP offerings are.

incorporating a VoIP component, such as AOL Instant Messenger or Microsoft Messenger? Given the fluid nature of market competition between telecommunications and information services, it would be inappropriate to establish a presumption of CALEA coverage for any product or service thought to compete with an existing, CALEA-covered product or service. Accordingly, the Commission has already adopted criteria that it would use in determining which entities and services are subject to CALEA, criteria that observe the distinction the Commission drew between covered telecommunications services and exempt information services.[26] Moreover, as discussed above, the Petitioners fail to explain why their existing ability to access the networks of underlying telecommunications carriers is insufficient to meet their needs to access the identifying information and content of information service traffic carried over those telecommunications networks.

Rather than extend CALEA's assistance capability requirements wholesale to information service providers, contrary to the clear statutory prohibition in CALEA, the needs of law enforcement and the needs of the telecommunications industry would be better served by working to implement the existing CALEA requirements for packet-mode intercept solutions by telecommunications carriers.

V. The Commission Should Reject Outright Petitioners' Proposed CALEA "Veto" Over the Deployment of New Technologies and Services

In various elements of their proposal, the Petitioners essentially propose a law enforcement "veto" over the deployment of new technologies and services lacking an intercept solution deemed CALEA-compliant by law enforcement. Specifically, the Petitioners seek FCC rules prohibiting service providers from deploying new

[26] *See Second Report and Order* at para. 14.

technologies or services without a CALEA intercept solution in place.[27] Furthermore, the Petitioners would require any service provider claiming exempt status under CALEA for any new service (for example, an information service) to first seek a declaratory ruling from the Commission that its service does not fall under CALEA before being able to deploy its new service.[28]

Given the Petitioners' blurring of the line between covered telecommunications services and exempt information services, it is easy to see why these elements of the Petitioners' proposal are unworkable. They would dramatically chill the deployment of new products and services by service providers exempt from CALEA's requirements. They would also force telecommunications carriers to refrain from deploying new telecommunications service technologies, even to serve nascent niche markets, until industry standard intercept solutions were readily available for those technologies. Indeed, imagine what broadband deployment would look like today if this proposal had been adopted by the Commission in the 1999 *Third Report and Order* – there wouldn't be any broadband deployment today.

There is simply no basis for creating a new regulatory hoop for providers of new technologies and services to jump through prior to deploying their services. For the alleged future omissions of some carriers to deploy intercept solutions pursuant to their existing statutory requirements, the Petitioners would punish the entire industry by forcing all service providers to choose between either "clearing" their service offerings with the Commission prior to deploying or waiting to deploy their service and technologies until the industry develops an intercept solution. In other words, for the

[27] *See* Joint Petition at 33-34 and 54-55.

[28] *See* Joint Petition at 54.

hypothetical sins of the few carriers in the future who fail to meet their CALEA obligations, the Petitioners would punish the many – by presuming all providers and services "guilty until proven innocent."

What is particularly puzzling is the absence of any compelling need for creating such a regime. Indeed, all telecommunications carriers, from the moment CALEA was passed into law, have been under a present, effective obligation to provide intercept assistance capabilities to law enforcement agencies for all of their equipment, facilities or services. Furthermore, from the moment CALEA was passed into law, all telecommunications carriers have been subject to enforcement action, for example under section 208 of the Communications Act, for failures to comply with their CALEA obligations. The Petitioners may contend that, while these existing obligations are all well and good, they have not been sufficiently enforced, which may or may not be a fair point. But, in any event, any supposed slackness in enforcing telecommunications carriers' existing CALEA obligations is no grounds for creating new obligations. Rather, the solution would be better enforcement of the existing CALEA obligations.

All telecommunications carriers are already under a present obligation to offer technical assistance capabilities for their equipment, facilities or services. Accordingly, the Commission should reject the Petitioners' proposals to presume the applicability of CALEA assistance capability requirements at the time any new technology or service is deployed, as well as the proposal to require service providers to pre-clear exempt new services and technologies with the Commission prior to deploying them. These proposals only burden exempt service providers with assistance capability requirements to which they should not be subject, and force telecommunications carriers to slow-roll their new

services and technologies to wait for intercept industry standards to be worked out. Given the general subpoena powers law enforcement retains to access such nascent services, it simply makes no sense to burden covered telecommunications carriers in this way.

VI. Instead of Adopting the Petitioners' Arbitrary Compliance Deadlines, the Commission Should Ensure that a Packet-Mode Intercept Solution is Standardized Soon

Covad urges the Commission to reject the Petitioners' call for a new 15 month implementation schedule for packet-mode CALEA intercept solutions, as well as similar benchmarks and deadlines for all new technologies and services on a going-forward basis.[29] What is needed now is not the imposition of arbitrary deadlines upon members of the industry. Rather, what's needed is the Commission's guidance and facilitation of a speedy conclusion to the standards-setting work already begun for packet-mode intercept solutions. After all, the Commission originally scheduled carriers to complete this work within 15 months back in 1999, when it first adopted packet-mode assistance capability requirements. Today, nearly 5 years later, this extensive process is finally nearing completion. Given this history, to think that all carriers could implement CALEA intercept solutions for all packet-mode services within a 15 month timeframe is highly doubtful.

Rather than simply setting an arbitrary deadline, sitting back, and waiting for adoption of an industry standard to develop, the Commission should take this opportunity to make itself an active participant in facilitating the speedy adoption and deployment of industry standards for packet-mode intercept solutions. The Telecommunications

[29] *See* Joint Petition at 40-57.

Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS) recently announced their release of published standards for lawfully authorized electronic surveillance, in a revised version of the "J-standard" (J-STD-025-B).[30] According to their announcement, "The details of the solution for the cdma2000 packet data system are included in the standard, as are normative references for Voice over Packet (VoP) for Wireline Telecommunications Networks and Universal Mobile Telecommunications System/General Packet Radio Service (UMTS/GPRS)…".[31] Their work, now culminated in a published standard, demonstrates that the industry standards setting process is working, and should not be bypassed or shortcut in favor of the imposition of an arbitrary set of deadlines.

Moreover, imposing an arbitrary 15 month deadline for packet-mode compliance by technologies and services not yet included in revisions to the J-standard would make little sense. Rather than bypass or shortcut the industry standards-setting process, the Commission should be encouraging it. It would be wasteful and burdensome indeed for carriers to rush to deploy an individual set of packet-mode intercept solutions, only to have to redo all that work (in order to fall within section 1006's safe harbors) when industry standards later emerged.[32] The effect of the Petitioners' proposed benchmarks and deadlines, particularly for services and technologies not yet included in packet-mode revisions to the J-standard, would be essentially to make them do the work of deploying packet-mode intercept solutions twice. In turn, forcing carriers to rush to deploy

---

[30] *See* "TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Standard (J-STD-025-B)," Press Release, Mar. 19, 2004, http://www.tiaonline.org/media/press_releases/index.cfm?parelease=04-26.

[31] *Id.*

[32] *See* 47 U.S.C. § 1006 (creating industry standard "safe harbors" for CALEA's assistance capability requirements).

individual, proprietary intercept solutions would remove much of the impetus for standards setting bodies to expend the time and resources necessary to develop industry standard solutions at all.

Accordingly, Covad urges the Commission to support the industry standards setting process for packet-mode intercept solutions under CALEA, rather than abandon that process in favor of an arbitrary set of deadlines. The industry standards-setting process is working. The Commission has a vital role to play in ensuring that it continues to work fairly and for the benefit of all parties involved, and in ensuring that new industry standards for CALEA intercept solutions are rapidly deployed by carriers as they emerge.

VII. Contrary to Petitioners' Assertions, CALEA Implementation Costs Can and Should be Borne by Law Enforcement Agencies under the OCCSSA

Finally, Covad takes issue with the Petitioners' construction of section 109(b) of CALEA as evincing Congressional intent to preclude carriers from recovering their costs of implementing CALEA assistance capabilities through their intercept provisioning charges to law enforcement under Title III of the Omnibus Crime Control and Safe Streets Act ("OCCSSA").[33] Contrary to the Petitioners' contentions, section 109(b) does not evince unmistakable Congressional intent to preclude carriers from recovering their CALEA implementation costs from law enforcement. To the contrary, section 109(b) merely establishes a vehicle for law enforcement to "purchase" post-January 1, 1995 measures to implement CALEA in the specific circumstances where the Commission deems those implementation measures to be not "readily achievable" by a given carrier.[34] For any non-readily achievable implementation measures sought by law enforcement,

[33] *See* Joint Petition at 64 (citing "47 U.S.C. § 109(b)" (sic), apparently a citation to 47 U.S.C. § 1008)(b)). *See also* 18 U.S.C. §§ 2510-2522 (codifying provisions of the OCCSSA).

[34] *See* 47 U.S.C. 1008(b).

where law enforcement refuses to pay for implementing such measures, carriers are absolved of any liability under 47 U.S.C. § 1002 for not implementing such measures.[35] In other words, section 109(b) creates an additional payment mechanism for carriers where law enforcement seeks CALEA implementation measures "above and beyond" carriers' ordinary duties. Section 109(b) says nothing at all, however, about what mechanisms for CALEA implementation cost recovery are in place for post-January 1, 1995 implementation measures that are "readily achievable."

Thus, section 109(b) does nothing to alter the compensation mechanisms already in place for CALEA implementation measures "readily achievable" by carriers. In other words, CALEA does nothing to alter the general rule that carriers' costs of providing court-ordered intercepts, including the capital costs of creating capabilities to provide such intercepts, should fall on law enforcement.[36] Indeed, the same provision of OCCSSA that creates this payment obligation specifically references and includes intercept orders under CALEA.[37] This is precisely the principle the Commission recognized in the *CALEA Order on Remand*, when it recognized that carriers could recover "at least a portion of their CALEA software and hardware costs by charging [to law enforcement agencies], for each electronic surveillance authorized by CALEA, a fee that includes recovery of capital costs…".[38] Contrary to the Petitioners' contentions, this statement hardly constituted an unauthorized rulemaking without notice and comment in

---

[35] *See* 47 U.S.C. 1008(d).

[36] *See* 18 U.S.C. § 2518(4).

[37] *See id.*

[38] *See Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896, 6917, ¶ 60 (2002) (*CALEA Order on Remand*).

violation of the Administrative Procedures Act.[39] Rather, this statement was simply a restatement, or at best a clarification, of the understanding known to exist all along – that Title III of the OCCSSA generally authorizes carriers to recover their intercept provisioning costs, including capital costs, from law enforcement. Section 109(b) does nothing to change this, but merely provides an additional payment mechanism for the burdensome costs "above and beyond" the call of readily achievable duties. It is the Petitioners' proposal to preclude carriers from recovering their capital costs for intercept provisioning from law enforcement which would require the creation of a new rule under the APA – a new rule in direct violation of the OCCSSA.[40]

Accordingly, Covad urges the Commission to reject the Petitioners' proposal to prohibit carriers from recovering their lawful intercept provisioning costs, including a reasonable pro-rata portion of their capital costs for implementing CALEA assistance capabilities, from law enforcement.

VIII. Conclusion

The Petitioners' proposals surely constitute an unwarranted and overreaching interpretation of CALEA, at the expense of carriers, their customers, and the innovative new broadband services now poised to drive the economy forward. Many of the Petitioners' proposals appear to be reincarnations of previous policy positions rejected by the Commission during its earlier CALEA proceedings. Also troubling is that, as explained above, it seems that the legitimate needs of law enforcement for access to new broadband networks could be accomplished with much narrower measures than what the Petitioners propose, including the simple enforcement of the interim packet-mode

[39] *See* Joint Petition at 69.

[40] *See* 18 U.S.C. § 2518(4).

requirements already in place, and facilitation of industry standards setting and adoption for packet-mode intercept capabilities. Accordingly, Covad urges the Commission to reject the expansive, burdensome proposals put forward by the Petitioners, and instead adopt the more moderate measures suggested herein.

Respectfully submitted,

/s/ Praveen Goyal

Praveen Goyal
Senior Counsel for Government & Regulatory Affairs

Covad Communications Company
600 14th Street, N.W.
Washington, D.C. 20005
202-220-0400 (voice)
202-220-0401 (fax)

April 12, 2004